



OSINT + ARCO + PROTECCIÓN DE DATOS

MAPA-RD: Exposición y Ruta de Cierre

Así se ve tu entorno digital desde fuera. Esto es lo que hay que cerrar primero.

MAPA-RD identifica exposición real (visible públicamente), prioriza riesgos y entrega una ruta de cierre ejecutable. Incluye base operativa para gestión ARCO y un esquema mensual de control continuo.

Sin auditorías genéricas. Sin promesas vacías.

ACME Corp · Reporte RPT-2026-001 · 2026-01-11

Executive Security Report · Exposición pública · Confidencial

Índice de Riesgo Digital

65

RIESGO CRÍTICO

VECTORES DE VULNERABILIDAD

ACTIVO:
Production Database
(AWS RDS)

TIPO:
Cloud Infrastructure

EXPOSICIÓN:
Public Repo Leak

DESCRIPCIÓN DEL EVENTO

Hardcoded credentials for the primary production database were identified in a public GitHub repository (config.js). Determining access logs confirmed unauthorized clone events.

IMPACTO

- Full compromise of customer data (PII).
- Potential total service disruption (Ransomware).
- Severe regulatory fines (GDPR/CCPA).

RUTA DE CIERRE

- Revoke the exposed AWS IAM credentials immediately.
- Rotate the database master password.
- Audit CloudTrail logs for suspicious activities since the commit date.
- Implement git-secrets to prevent future commits.

ACTIVO:
admin.acme.com

TIPO:
Web Application

EXPOSICIÓN:
Missing Control

DESCRIPCIÓN DEL EVENTO

The administrative panel allows single-factor authentication. Brute-force attacks or credential stuffing could easily compromise an admin account.

IMPACTO

- Unauthorized administrative access.
- Data manipulation or deletion.
- Backdoor installation.

RUTA DE CIERRE

- Enforce MFA (Time-based OTP) for all admin roles.
- Restrict access to VPN or trusted IPs only.
- Implement rate-limiting on the login endpoint.

ACTIVO:
dev.acme.com

TIPO:
Dev Environment

EXPOSICIÓN:
Configuration

DESCRIPCIÓN DEL EVENTO

The SSL certificate for the development environment is expired, triggering browser warnings and exposing traffic to interception.

RUTA DE CIERRE

1. Provision a new LetsEncrypt certificate.
2. Automate renewal via Certbot.

IMPACTO

- Developer workflow disruption.
- Man-in-the-Middle (MitM) risk if used externally.
- Loss of trust validation.

Anexo Técnico

Índice de Riesgo del Vector (IRV)

El **IRV** es la métrica fundamental de urgencia. No mide el riesgo teórico, sino la necesidad operativa de cierre. Se calcula internamente mediante un modelo ponderado de seis dimensiones.

FÓRMULA DE CÁLCULO

$$\text{IRV} = [\Sigma (\text{Componente} \times \text{Peso}) / \Sigma (\text{Peso Máximo})] \times 100$$

Variables del Modelo

Criticidad (CA)

x4

Importancia crítica del activo para la continuidad del negocio.

Exposición (ET)

x3

Ventana de tiempo y vigencia actual del hallazgo.

Superficie (SE)

x3

Facilidad de acceso desde redes públicas o privadas.

Impacto (IM)

x4

Suma de impactos (Financiero, Legal, Operativo, Reputacional).

Explotación (FE)

x3

Recursos y complejidad técnica requerida para el ataque.

Detección (DV)

x3

Probabilidad de evasión de sistemas de monitoreo.

Índice de Riesgo Digital (IRD)

El **IRD** es el indicador de postura global. Se deriva dinámicamente de los vectores activos mediante un promedio ponderado por severidad.

AGREGACIÓN PONDERADA

$$\text{IRD} = \frac{\sum (\text{IRV} \times \text{Peso Severidad})}{\sum (\text{Pesos Severidad})}$$

Matriz de Pesos

BAJO

Mult x1

MEDIO

Mult x2

ALTO

Mult x3

CRÍTICO

Mult x4

MÁXIMO

Mult x5